

S. AMANDA MARSHALL, OSB #95347  
United States Attorney  
District of Oregon  
**ETHAN D. KNIGHT**, OSB #99298  
**CHARLES F. GORDER, JR.**, OSB #91287  
Assistant United States Attorneys  
[ethan.knight@usdoj.gov](mailto:ethan.knight@usdoj.gov)  
[charles.gorder@usdoj.gov](mailto:charles.gorder@usdoj.gov)  
1000 S.W. Third Ave., Suite 600  
Portland, OR 97204-2902  
Telephone: (503) 727-1000  
Facsimile: (503) 727-1117  
Attorneys for United States of America

**UNITED STATES DISTRICT COURT**  
**DISTRICT OF OREGON**  
**PORTLAND DIVISION**

**UNITED STATES OF AMERICA**

**Case No. 3:12-CR-00659-MO**

**v.**

**REAZ QADIR KHAN,**

**Defendant.**

**GOVERNMENT'S RESPONSE TO  
DEFENDANT'S MOTION FOR ORDER  
ALLOWING DEFENSE COUNSEL  
ACCESS TO OTHERWISE *EX PARTE*  
PROCEEDINGS PURSUANT TO  
FISA OR CIPA**

The United States of America, by S. Amanda Marshall, United States Attorney for the District of Oregon, and through Ethan D. Knight and Charles F. Gorder, Jr., Assistant United States Attorneys, hereby responds to defendant's Motion for Order Allowing Defense Counsel Access to Otherwise *Ex Parte* Proceedings Pursuant to FISA or CIPA, ECF No. 68.

**I. STATEMENT OF FACTS**

On December 27, 2012, the grand jury returned an indictment charging defendant Reaz Khan with Conspiracy to Provide Material Support to Terrorists, in violation of Title 18, United

States Code, Section 2339A. (ECF No. 1). A three-week jury trial is scheduled to begin on April 13, 2015. A brief summary of the government's case follows.

At approximately 10:21 a.m. on May 27, 2009, a white Toyota van approached the entryway of the headquarters of the ISI<sup>1</sup> in Lahore, Pakistan. Inside the van were three men. One of them was a Maldivian national named Ali Jaleel. As the van approached the building, its occupants began to exchange fire with armed guards. After a brief exchange, a bomb in the van was detonated. The blast killed approximately 30 people and injured 300 more.

In a video released by As Sahab (the media outlet of Al Qaida) several months after the attack, Jaleel can be seen preparing for the attack at a training camp in what appears to be the Federally Administered Tribal Area (FATA) of Pakistan. In the video, Jaleel stated his motivation for the attack:

I want my blood to be the bit of carpet . . . the red carpet which will take the ummah<sup>2</sup> to its glory. So this carpet has been contributed with many bloods. . . . So I want to be among that caravan so that I can be a brick upon which Islam will stand.

Several years before his 2009 attack, Jaleel had attempted to reach Pakistan to train for violent jihad. In April 2006, Jaleel and several of his associates were stopped by Sri Lankan authorities as they attempted to board a plane to Qatar at the Colombo International Airport in Sri Lanka. Authorities later learned that Jaleel and the others had been attempting to fly to Pakistan in the hopes of traveling to Iraq or Afghanistan for the purposes of committing jihad.

---

<sup>1</sup> "ISI" is the acronym for the Directorate for Inter-Services Intelligence, one of the intelligence agencies of the government of Pakistan.

<sup>2</sup> Ummah is an Arabic word meaning "the Islamic nation."

Jaleel later told an FBI agent that his plan to get to Iraq or Afghanistan was not well thought out and that he “lacked a contact” in Pakistan.

Defendant Khan is a United States citizen who was born in Pakistan and currently resides in Portland, Oregon. Defendant Khan and Jaleel were long-time friends. In the fall of 2008, Jaleel urgently reached out to defendant Khan seeking his help to travel to Pakistan. On October 23, 2008, defendant Khan emailed Jaleel detailed advice on traveling to Pakistan and indicated the he (defendant Khan) could arrange for Jaleel to pick up money in Pakistan which Jaleel needed to get into a terrorist training camp to attain his goal of waging jihad.

On October 26, 2008, Jaleel wrote to defendant Khan that he had to “be in pak within this week... So I am to go there straight with the risk, this due to the place where my study is; there is a delegate from there and he awaits me there and he asked me to come within this week so I can join in this semester.” Jaleel indicated that he needed “2500 for everything.” The evidence will show that Jaleel’s references in this email to “study” and “semester,” as well as other references to “college,” were code words Jaleel used to thinly disguise his plans to attend a terrorist training camp in Pakistan.

Defendant Khan also provided advice and financial assistance to Jaleel’s family, knowing that his friend might die in an effort to commit violent jihad. In the course of their communications, Jaleel made it clear that he would not be returning to the Maldives and was worried about his family. As a result, defendant Khan volunteered to care for Jaleel’s family.

///

///

On October 26, 2008, Jaleel wrote:

My wife and kids.... once they are out of there, there is no going back... they have no options... no family to return to... once they are with you must take them as your own, educate them as your own... do not abandon [sic] them even in your worst difficulties, and do take them where your family goes... Educate them and bring them up well... please.

Defendant Khan's response made it clear that he understood that Jaleel would not see his family again and that he accepted the responsibility conferred on him:

I understand your worries about your family. Put your reliance and trust in Allah, He is the real Helper and Supporter. InshaAllah, Bi idhnillahi wa Aounihi [God willing, with God's permission and his help], I will try to support them as much as possible. So make duas [prayers] that Allah makes it possible and easy for me.

Defendant Khan arranged through a business associate in the United States to have a second person in Karachi, Pakistan, provide \$2500 to Jaleel. On November 3, 2008, defendant Khan sent Jaleel directions on how to pick up the money from a "trusted brother." Defendant and Jaleel continued to communicate until November 8, 2008, at which time Jaleel had successfully reached Pakistan and presumably picked up the money.

Sometime later, the defendant's business associate in the United States was called by his contact in Pakistan who had facilitated the delivery of the money to Jaleel for defendant Khan. The U.S. business associate was informed that his Pakistani contact had been visited by the local authorities and questioned about the transaction with Jaleel. The U.S. business associate became worried and contacted defendant Khan, who told him that the money was for a friend whose wife was sick.

///

After defendant Khan and Jaleel had their last known contact with one another, defendant took a number of steps to assist Jaleel's family. Defendant Khan and his wife were in frequent communication with Jaleel's wives and another individual in the Maldives in a continuing effort to provide support and advice to Jaleel's family. Jaleel made it clear through one of his wives that he appreciated defendant Khan's assistance. On June 2, 2009, six days after Jaleel's suicide attack in Pakistan, defendant Khan wired \$750 from a Fred Meyer store in Tigard, Oregon, to one of Jaleel's wives in the Maldives.

As the Court is aware, the government has filed notices in this matter that it intends to offer into evidence or otherwise use or disclose in this proceeding information derived from the acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter "FISA"). (*See* ECF No. 7 and ECF No. 59). Citing the unremarkable proposition that this case will therefore likely involve classified information to be provided by the government to the Court in the future, the defendant seeks an order that defense counsel be granted access to the government's future classified submissions.<sup>3</sup> Because the well-settled rule in criminal cases is that classified information provided to the Court under either provisions of the Classified Information Procedures Act, Title 18, U.S.C. app. 3 (hereinafter "CIPA"), or during FISA litigation under Title 50, U.S.C. §1806(f) is almost always done so *ex parte*, the defendant's motion should be denied.

---

<sup>3</sup> Defendant limits his request at this time to what he assumes will be a classified response to his pending motion regarding the interception of privileged communications (ECF No. 64), but he also makes clear on page 2, note 1, of the instant motion that this request for access to classified pleadings filed by the government will be a "recurring" one. The government intends this response to answer the defendant's claim for access to classified information in all future classified pleadings.

## II. ARGUMENT

### A. Whether to Classify Information and the Proper Classification Thereof Is a Matter Committed Solely to the Executive Branch.

The government has a “‘compelling interest’ in withholding national security information from unauthorized persons in the course of executive business.” *Dep’t of Navy v. Egan*, 484 U.S. 518, 527 (1988). As the Supreme Court has repeatedly stressed, courts should be “‘especially reluctant to intrude upon the authority of the Executive in . . . national security affairs.” *Egan*, 484 U.S. at 530; *see also Haig v. Agee*, 453 U.S. 280, 307 (1981) (protecting the secrecy of our government’s foreign intelligence operations is a compelling interest); *CIA v. Sims*, 471 U.S. 159, 168–69 (1985) (the Director of Central Intelligence has very broad authority to protect all sources of intelligence information from disclosure). Accordingly, courts have recognized that the determination of whether to classify information and the proper classification thereof is a matter committed solely to the Executive Branch: “The Government . . . may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it.” *United States v. Smith*, 750 F.2d 1215, 1217 (4th Cir.), *vacated on other grounds*, 780 F.2d 1102 (4th Cir. 1985).

In his supporting memorandum, defendant Khan pays lip service to the procedures of both CIPA and FISA, but seemingly ignores the effect of those statutes. He simply indicates that one of his three attorneys currently has an active Secret-level security clearance received in the past during unrelated litigation and offers that she and her co-counsel are all willing to seek and obtain similar clearances in this case. (Def.’s Mot., Ex. A, ¶¶ 2, 8; ECF No. 68-1 at 3-4).

///

But even if defense counsel had appropriate security clearances, a clearance alone does not entitle them to access the government's classified files or its classified pleadings. To obtain access to classified information, one also has to have a need to access such information. Exec. Order No. 13526, § 4.1(a)(3), 75 Fed. Reg. 707, 720 (Dec. 29, 2009). Such a need is not established simply because counsel is representing a defendant.

In *United States v. Sedaghaty*, 728 F.3d 885, 908 (9th Cir. 2013), the Ninth Circuit once again reiterated this principle, holding that a challenge to *ex parte* proceedings involving classified information from which cleared counsel were excluded was “a battle already lost in the federal courts.”

[T]he simple fact that defense counsel held security clearances does not mean that the attorneys were entitled to access the government's classified filings.

*Id.* at 909. Accord *United States v. Bin Laden*, 126 F. Supp. 2d 264, 287 n.27 (S.D.N.Y. 2000), *aff'd*, *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008). See also *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987) (explaining, in the FISA context, that “Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated”); *United States v. El-Mezain*, 664 F.3d 467, 568 (5th Cir. 2011) (approving denial of FISA discovery to cleared defense counsel given the government's substantial interests in maintaining secrecy of the materials), *cert. denied*, 133 S. Ct. 525 (2012); *United States v. Abu Ali*, 528 F.3d 210, 253 (4th Cir. 2008) (“[W]e have no authority[ ] to consider judgments made by the Attorney  
///

General concerning the extent to which the information in issue here implicates national security.”).

**B. CIPA Section 4 and Rule 16(d)(1) Permit the Court to Examine Classified Information Provided *Ex Parte* by the Government and to Restrict Access to Such Information by the Defense.**

CIPA governs how federal courts address and process pretrial matters concerning the discovery, admissibility, and use of classified information in criminal cases. *See United States v. Baptista-Rodriguez*, 17 F.3d 1354, 1363 (11th Cir. 1994). “Congress intended section 4 [of CIPA] to clarify the court’s powers under Fed. R. Crim. P. 16(d)(1) to deny or restrict discovery in order to protect national security.” *United States v. Sarkissian*, 841 F. 2d 959, 965 (9th Cir. 1988). CIPA’s fundamental purpose is to “harmonize a defendant’s right to obtain and present exculpatory material upon his trial and the government’s right to protect classified material in the national interest.” *United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996) (quoting *United States v. Wilson*, 571 F. Supp. 1422, 1426 (S.D.N.Y. 1983)); *see also United States v. Apperson*, 441 F.3d 1162, 1193 n.8 (10th Cir. 2006). “CIPA does not expand or restrict established principles of discovery . . . .” *Sedaghaty*, 728 F.3d at 903.

Section 4 of CIPA and Rule 16(d)(1) authorize a district court to deny or otherwise restrict discovery of classified information by the defense. Section 4 of CIPA provides, in pertinent part, that a district court:

upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a



statement admitting relevant facts that the classified information would tend to prove.

18 U.S.C. app. 3, § 4; *see also* Fed. R. Crim. P. 16(d)(1) (a district court “may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief”). While courts have discretion to consider the need for a protective order in any criminal case, CIPA specifically focuses on how courts should exercise that discretion when classified information is at issue. *See, e.g., Sarkissian*, 841 F.2d at 965. And under Section 4 and Rule 16(d)(1), the Court may authorize the government to withhold entirely from discovery classified materials that are not properly discoverable under the appropriate legal standard. *United States v. Yunis*, 867 F.2d 617, 624–25 (D.C. Cir. 1989); *United States v. Libby*, 429 F. Supp. 2d 46, 48 (D.D.C. 2006).

In sum, even cleared counsel would not have a need to know the classified information submitted to the Court in connection with the government’s CIPA Section 4 motions, unless the Court rules that the classified information is discoverable. Once discoverable, defense counsel would still not need a security clearance unless there were no options to disclosure of the classified information itself available to the government under CIPA (such as substitution), and the government was unable to declassify the information. This case has not reached such a stage and thus the clearance status of defense counsel is irrelevant. Moreover, the government currently intends to provide all discoverable information in this case to the defense in an unclassified form. Thus, security clearances for defense counsel would not become necessary or relevant.

///

///

**C. FISA Does Not Contemplate Automatic Access to FISA Materials by Defense Counsel.**

As this Court is well aware from other cases in this district, the government's long-standing practice is not to declassify or make available the pleadings filed with the Foreign Intelligence Surveillance Court ("the "FISC") to defense counsel, even if defense counsel possesses a security clearance. *See, e.g., United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167 (D. Or. Apr. 21, 2010). The government will more specifically respond to any request for access to any FISC pleadings or orders in this matter when and if it responds to any future motion to suppress evidence obtained pursuant to FISA. Such a government response is not even due to be filed until December 8, 2014, and thus any request for access to FISC material at this point is premature. *See generally* 50 U.S.C. §§ 1806(f) and 1825(g).

In assessing the legality of FISA-authorized electronic surveillance, physical searches, or both, the district court, "shall, notwithstanding any other law, if the Attorney General files an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g).

On the filing of the Attorney General's affidavit or declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] *only where such disclosure is necessary* to make an accurate determination of the legality of the surveillance

[or search].”<sup>4</sup> 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). Thus, the propriety of the disclosure of any FISA applications or orders to the defense cannot even be considered unless and until the Court has first concluded that it is unable to make an accurate determination of the legality of the collection after reviewing the government’s submissions (and any supplemental pleadings that the Court might request) *in camera* and *ex parte*. See *El-Mezain*, 664 F.3d at 565; *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010); *Nicholson*, 2010 WL 1641167, at \*4 (“After an *in-camera* review, the court ‘has the discretion to disclose portions of the documents, under appropriate protective procedures, *only if [the court] decides that such disclosure is necessary to make an accurate determination of the legality of the surveillance.*’” (quoting *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984))).

If the Court is able to make an accurate determination of the legality of any FISA electronic surveillance or physical searches based on its *in camera*, *ex parte* review of the materials submitted by the United States, then the Court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *El-Mezain*, 664 F.3d at 566; *Abu-Jihaad*, 630 F.3d at 129; *Duggan*, 743 F.2d at 78.

Federal courts have repeatedly and consistently held that FISA “anticipates that an *ex parte*, *in camera* determination is to be the rule,” with disclosure and an adversarial hearing being the “exception, occurring *only* when necessary.” *United States v. Belfield*, 692 F.2d 141,

---

<sup>4</sup> In *United States v. Warsame*, 547 F. Supp. 2d 982 (D. Minn. 2008), the court addressed the meaning of “necessary” in this context, noting that “[t]he legislative history explains that such disclosure is ‘necessary’ only where the court’s initial review indicates that the question of legality may be complicated” by factual misrepresentations, insufficient identification of the target, or failure to comply with the minimization standards in the order. 547 F. Supp. 2d at 987.

147 (D.C. Cir. 1982); *see also El-Mezain*, 664 F.3d at 567 (“[D]isclosure of FISA materials ‘is the exception and *ex parte*, *in camera* determination is the rule.’” (quoting *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009))); *Nicholson*, 2010 WL 1641167, at \*3-4; *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. 1989), *aff’d*, 958 F.2d 365 (3d Cir. 1992) (“It is well established that the legality of foreign intelligence surveillance should be determined on an *in camera*, *ex parte* basis.”).

In fact, with one exception,<sup>5</sup> every court which has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion about the legality of the FISA collection at issue based solely on its *in camera*, *ex parte* review. The government is confident that in this matter, should a motion to suppress FISA evidence be ultimately filed, that this Court will similarly be able to make its determination based upon its *in camera*, *ex parte* review without the need for an adversary hearing.

///

///

///

///

///

///

///

---

<sup>5</sup> Earlier this year, a district court ordered disclosure of FISA material in *United States v. Dauod*, No. 12-CR-723, 2014 WL 321384 (N.D. Ill., filed January 29, 2014). That order is currently on appeal to the Seventh Circuit Court of Appeals, *United States v. Daoud*, No. 14-1284).

### III. CONCLUSION

For the reasons give below, the defendant's motion for an order allowing defense counsel access to otherwise *ex parte* proceedings pursuant to FISA or CIPA should be denied.

Dated this 12th day of May 2014.

Respectfully submitted,

S. AMANDA MARSHALL  
United States Attorney

*s/ Charles F. Gorder, Jr.*  
ETHAN D. KNIGHT, OSB #99298  
CHARLES F. GORDER, JR., OSB #91287  
Assistant United States Attorneys  
(503) 727-1000